Large Automotive Supplier

After a series of acquisitions sparked sharp increases in both the number of IT systems and employees, this company realized that manual management of access rights was no longer viable. The firm introduced NetIQ® Identity Manager, enabling it to automatically grant blue- and white-collar workers alike role-based access to the information they require to fulfill their relevant tasks.

Overview
This company is a large supplier serving companies in the automotive industry. It achieves multi-billion-dollar annual revenues and employs hundreds of thousands of people spread all over the globe.

Challenge
In the automotive industry, competition is extremely fierce and innovation is the differentiator. Vehicle manufacturers and their suppliers must therefore protect their intellectual property by ensuring that workers can access only the information that is relevant to their roles, and that user access is terminated for former staff as soon as they leave the company.

In the past, this firm had managed access rights for all of its blue- and white-collar workers plus external staff manually. But the number of business systems and employees increased each time the firm acquired a smaller company, making access management very cumbersome. To make matters more complicated, each staff member requires access to a different subset of systems depending on his or her role.

Ultimately, manually managing access for so many users became unviable due to the excessive amount of work that it involved. That’s when the company began looking for a better alternative.

Solution
The IT department aimed to unleash the maximum possible value from its identity management solution by choosing one that could integrate with all of the company’s business systems. After evaluating offerings from a range of providers, the company decided to deploy Identity Manager because it offered seamless integration with SAP software, which the firm uses to manage a huge share of its business processes.

As a first step towards centralized identity management, the company set up a single global HR system. The IT team then began a clearing process aimed at matching up employee identities across the HR system, IBM Notes, Microsoft Active Directory and multiple SAP systems.

Next, the company began implementing Identity Manager to provide centralized management for hundreds of thousands of employee accounts and access to critical systems.

Results
+ Automated and accelerated the provisioning and deprovisioning of user accounts for new and former employees
+ Provided a clearer overview of access rights
+ Introduced role-based provisioning

At a Glance

- **Industry**: Automotive
- **Location**: Undisclosed
- **Challenge**: Complex manual identity management processes were becoming cumbersome as the supplier continued to grow.
- **Solution**: Use Identity Manager to provide centralized management for hundreds of thousands of employee accounts and access to critical systems.

Customer Success Story

Large Automotive Supplier

After a series of acquisitions sparked sharp increases in both the number of IT systems and employees, this company realized that manual management of access rights was no longer viable. The firm introduced NetIQ® Identity Manager, enabling it to automatically grant blue- and white-collar workers alike role-based access to the information they require to fulfill their relevant tasks.
management. Identity Manager features roles-based provisioning, which enables the company to automatically grant new employees access to the relevant subset of systems depending on their jobs.

**Results**

The company is confident that the implementation of Identity Manager will slash the amount of time needed to provision accounts for new hires, thus allowing them to make valuable contributions to the company from day one.

Similarly, the solution will enable the company to automate and accelerate the deprovisioning of user accounts for employees leaving the organization. This will help to ensure that former staff can no longer access confidential information, reducing the risk of intellectual property loss.

“Introducing Identity Manager will free our IT staff from manual user administration, enabling them to focus on value-add initiatives,” said a company spokesperson.

Identity Manager will give the company a much clearer overview of access rights and greater control in providing all users with access to the systems they need according to their roles.

Having a clear view of which employees can access which systems is important not only for meeting compliance requirements around security, but also because it helps the company to save money by paying for only the software licenses that it needs.

In the future, the company is planning to introduce single sign-on for its users, reducing the number of passwords that employees need to remember. Staff will be able to manage their passwords without help from the IT department, which will cut the number of password-related calls to the IT helpdesk.

The firm is confident that Identity Manager will bring enormous value to its business by eliminating manual work, driving greater value from its IT department and ramping up protection of its intellectual property.

“Introducing Identity Manager will free our IT staff from manual user administration, enabling them to focus on value-add initiatives.”

**SPOKESPERSON**
Large Automotive Supplier

www.netiq.com